

Datenschutz im Betrieb: Das Wichtigste auf einen Blick

Datenschutzgrundlagen für den Betriebsrat

Das Datenschutzrecht ist nicht immer einfach zu überblicken – egal, ob es um Vorschriften der Datenschutzgrundverordnung (DSGVO) oder des Bundesdatenschutzgesetzes (BDSG) geht. Wir haben Ihnen die wichtigsten Regelungen zu den drängendsten Fragen im Betriebsrat zusammengestellt.



Stephan Sägmüller | ifb

Stand: 1.2.2024

Lesezeit: 03:00 min



© AdobeStock | MT.PHOTOSTOCK

Wann, wo und für wen gilt die DSGVO?

Art. 2 DSGVO dient der Bestimmung des sogenannten sachlichen Anwendungsbereichs. Danach gilt die DSGVO für die ganz oder teilweise Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Bei dieser recht „sperrigen“ Definition ist es wichtig, die Begrifflichkeiten der DSGVO zu kennen und richtig einordnen zu können. Hier hilft Art. 4 DSGVO weiter.

Beispiel: Handelt es sich um keine personenbezogenen Daten, so ist die DSGVO auch nicht anwendbar.



Wichtig: Eine Ausnahme bildet hierzu Art. 2 Abs. 2 DSGVO. Insbesondere Art. 2 Abs. 2 Nr. 3 DSGVO ist hier regelmäßig zu beachten. Danach findet die DSGVO keine Anwendung auf natürliche Personen, die ausschließlich persönliche oder familiäre Tätigkeiten ausüben. Damit unterliegt der private bzw. familiäre Lebensbereich konsequenterweise nicht der Kontrolle der Verordnung

Wo gilt die DSGVO?

Die beiden wichtigsten Anwendungsbereiche unterscheiden sich wie folgt:

- Es existiert eine Niederlassung des Verantwortlichen innerhalb der EU (Art. 3 Abs. 1 DSGVO): Die DSGVO ist anwendbar, unabhängig vom tatsächlichen Ort der Datenverarbeitung. **Beispiel:** Der Betrieb des Arbeitgebers befindet sich innerhalb der EU.
- Es existiert keine Niederlassung des Verantwortlichen innerhalb der EU (Art. 3 Abs. 2 und 3 DSGVO): Die DSGVO ist anwendbar, wenn sich die betroffenen Personen (auch nur kurzfristig) innerhalb der EU aufhalten, unabhängig von der Staatsangehörigkeit bzw. des Status als Unionsbürger und die Datenverarbeitung im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen steht (ein konkretes Angebot ist nicht erforderlich). **Beispiel:** Der Betrieb des Arbeitgebers befindet sich außerhalb der EU, sein Dienstleistungsangebot erstreckt sich allerdings auch auf Bürger, die sich in der EU aufhalten.

Für wen gilt die DSGVO?

Grundsätzlich sind alle natürlichen Personen geschützt (Art. 1 DSGVO). Wichtig für das Arbeitsverhältnis ist auch § 26 BDSG, der spezifischere Vorschriften zum Beschäftigtendatenschutz enthält. Dabei erstreckt sich der Schutzbereich gem. § 26 Abs. 8 BDSG ausdrücklich neben Arbeitnehmern und weiteren auch auf Auszubildende, Leiharbeitnehmer und Bewerber. Insbesondere letztere befinden sich regelmäßig in einer gegenüber dem Arbeitgeber schwachen Position, sodass diese besonders schutzbedürftig sind.

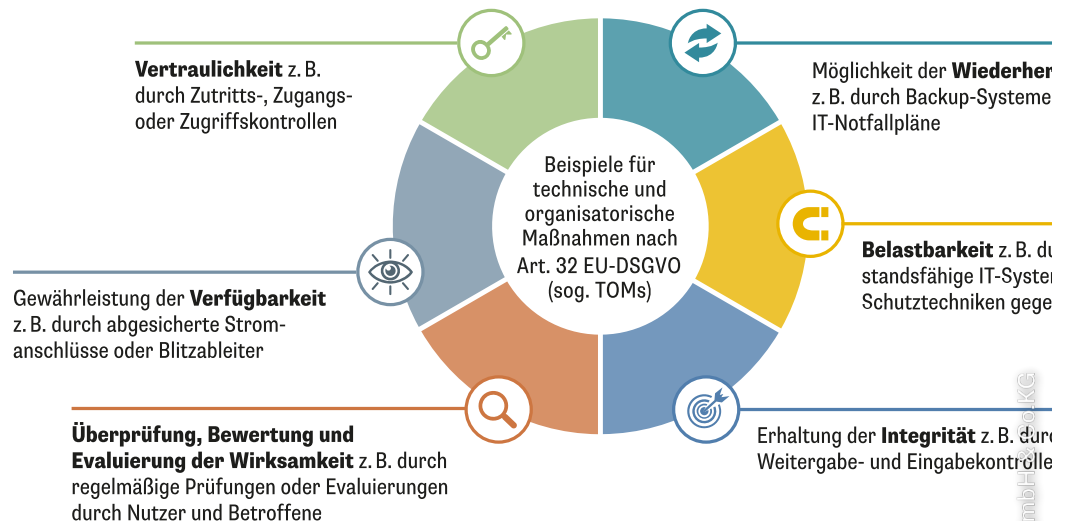
Datenschutzgrundsätze: Was muss bei der Datenverarbeitung beachtet werden?

Art. 5 DSGVO beschreibt die Grundsätze für die Verarbeitung von personenbezogenen Daten. So müssen Daten:

- auf rechtmäßige Weise, nach Treu und Glauben und in nachvollziehbarer Weise verarbeitet werden (Rechtmäßigkeit, Treu und Glauben, Transparenz),
- für legitime, festgelegte und eindeutige Zwecke verarbeitet werden (Zweckbindung),
- die Verarbeitung auf das notwendige Maß beschränkt werden (Datenminimierung),
- sachlich richtig und falls notwendig auf dem neuesten Stand sein (Richtigkeit),
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Speicherbegrenzung),

- auf eine Art und Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (Integrität und Vertraulichkeit).

Technische und organisatorische Maßnahmen



Auch wenn Art. 5 DSGVO keine explizite Regelung zur Verpflichtung der Mitarbeiter auf das Datengeheimnis enthält, ist diese weiterhin unerlässlich. Die Verpflichtung auf das Datengeheimnis als solche ist in Art. 5 DSGVO zwar nicht mehr vorhanden, auf das Datengeheimnis wird jedoch an verschiedenen Orten der DSGVO Bezug genommen. Der Wegfall der Regelung sollte daher nicht dazu verleiten, fortan von Verpflichtungserklärungen Abstand zu nehmen. Ganz im Gegenteil: Auch weiterhin muss eine Verpflichtungserklärung der Mitarbeiter auf das Datengeheimnis erfolgen.

Wann dürfen personenbezogene Daten verarbeitet werden?

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach Art. 6 DSGVO nur dann zulässig, soweit:

1. dies entweder durch die DSGVO bzw. das BDSG selbst vorgesehen ist (z.B. § 26 BDSG),
2. eine andere Rechtsvorschrift (z.B. SGB, Tarifvertrag, Betriebsvereinbarung) dies erlaubt oder anordnet,
3. der Betroffene einwilligt (Art. 7 DSGVO, § 26 Abs. 2 BDSG), oder
4. zur Erfüllung eines Vertrages (selten der Fall).

Bei Art. 6 DSGVO spricht man von einer sogenannten Verbotsnorm mit Erlaubnisvorbehalt, da die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten und nur unter den oben genannten Kriterien zulässig ist. Da demzufolge der Arbeitgeber darlegen muss, warum er bestimmte Daten verarbeiten will, erleichtert dies die Arbeit des Betriebsrats. **Wichtig ist**, dass für jede Datenverarbeitung eine Rechtsgrundlage gegeben sein muss.

Beispiel BEM

„Andere Rechtsvorschriften“ im Sinne des Art. 6 DSGVO finden sich z.B. in den steuerrechtlichen Bestimmungen und in den Sozialgesetzbüchern. So ist etwa das in § 167 SGB IX geregelte betriebliche Eingliederungsmanagement eine andere Rechtsvorschrift in diesem Sinne.

Beim betrieblichen Eingliederungsmanagement hat der Arbeitgeber mit Beschäftigten, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, unter Beteiligung des Betriebsrats (und bei schwerbehinderten Menschen zudem unter Beteiligung der Schwerbehindertenvertretung) Möglichkeiten abzuklären, wie die Arbeitsunfähigkeit möglichst überwunden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt werden kann. Für die Durchführung dieses Verfahrens ist die Einwilligung des betroffenen Arbeitnehmers erforderlich (§ 167 Abs. 2 S. 1 SGB IX). Liegt diese vor, so ist § 167 Abs. 2 SGB IX gleichzeitig die Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung der Daten im Rahmen des betrieblichen Eingliederungsmanagements.

Vorschriften zur Sozialauswahl

Anders verhält es sich beispielsweise bei den Vorschriften zur Sozialauswahl. Nach § 1 Abs. 3 KSchG ist der Arbeitgeber bei betriebsbedingten Kündigungen zur Sozialauswahl verpflichtet. Die Regelung verpflichtet den Arbeitgeber zwar, die Sozialdaten zu erheben und den bzw. die weniger sozial schutzwürdigen Arbeitnehmer zu kündigen, jedoch folgt aus der Pflicht nicht gleichzeitig auch das Recht zur Datenerhebung. Das Recht zur entsprechenden Datenverarbeitung folgt hier nicht aus § 1 Abs. 3 KSchG, sondern aus § 26 BDSG. Damit ist § 1 Abs. 3 KSchG keine andere Rechtsvorschrift im Sinne des Art. 6 DSGVO.

Tarifverträge und Betriebsvereinbarungen

Auch Tarifverträge und Betriebsvereinbarungen können Erlaubnistatbestände im Sinne von Art. 6 EU-DSGVO sein. Das unterstreicht Art. 88 Abs. 1 EU-DSGVO auch nochmals und nennt hier Betriebsvereinbarungen bzw. Kollektivvereinbarungen ausdrücklich. Der Betriebsrat muss jedoch Betriebsvereinbarungen, die zu stark in das Datenschutzrecht bzw. die Persönlichkeitsrechte eingreifen, nicht zustimmen.

Unterstützen Sie Ihre Kollegen beim Thema Einwilligung und eigene Rechte

Eine weitere Art der Rechtfertigung ist die Einwilligung des betroffenen Beschäftigten in die Datenverarbeitung. Die Wirksamkeit einer Einwilligung hängt von einigen Bedingungen ab. Wichtig ist, dass eine Einwilligung vor einer Datenverarbeitung erfolgt, dem Betroffenen die Bedeutung und Tragweite bewusst ist, er ausreichende Informationen über den Zweck erhält und er sie höchstpersönlich, idealerweise schriftlich, abgibt, ohne hiervon weitere rechtliche Folgen abhängig zu machen.

Wann ist eine Einwilligung wirksam?

Eine wirksame Einwilligung liegt nur vor, wenn folgende Voraussetzungen nach Art. 4 Nr. 11 und 7 DSGVO, § 26 Abs. 2 BDSG erfüllt sind:

- Vorherige Einholung der Einwilligung (§ 183 BGB): Die Einwilligung muss eingeholt werden, bevor die Daten verarbeitet werden.

- Bedeutung und Tragweite des Betroffenen: Der betroffene Arbeitnehmer muss die Reichweite seiner Entscheidung erkennen können. Die Einwilligungsfähigkeit als solche liegt gem. § 104 BGB vor, wenn die betroffene Person älter als sieben Jahre und im Vollbesitz ihrer geistigen Kräfte ist. Beschränkt geschäftsfähig ist, wer zwischen sieben und 18 Jahre alt ist (ggf. Einwilligung des gesetzlichen Vertreters gem. § 108 BGB notwendig).
- Ausreichende Informationen des Arbeitgebers zum Zweck der Datenverarbeitung sowie ggf. über die Folgen der Verweigerung: Der betroffene Arbeitnehmer ist auf sämtliche Daten, auf die sich seine Einwilligung bezieht, hinzuweisen – auch auf den Zweck, sowie bei Datenübermittlung auf Zweck und Empfänger der Übermittlung. Eine Blankoeinwilligung ist nicht möglich.
- Höchstpersönlich: Die Einwilligung muss höchstpersönlich erfolgen. Eine Stellvertretung ist also nicht möglich. Wichtig: In diesem Punkt ist man sich nicht einig. Es wird ebenfalls die Meinung vertreten, die Einwilligung müsse nicht zwingend höchstpersönlich erfolgen. Tipp: Um Missverständnisse zu vermeiden, sollte der Betriebsrat im Arbeitsverhältnis auf eine höchstpersönliche Abgabe der Einwilligungserklärung achten.
- Koppelungsverbot: Gem. Art. 7 Abs. 4 DSGVO wird die Unfreiwilligkeit der Einwilligung angenommen, falls die Durchführung eines Vertrages von der Einwilligung in eine Datenverarbeitung abhängig gemacht wird, die für diesen Vorgang gar nicht notwendig ist.
- Schriftform: Eine Einwilligung in eine Datenverarbeitung ist grundsätzlich formfrei möglich, z.B. auch per Video. Auch im Arbeitsverhältnis ist eine elektronische Einwilligung möglich. Nur bis November 2019 galt im Arbeitsverhältnis eine strengere Vorschrift, wonach eine Einwilligung im Beschäftigungsverhältnis schriftlich abzugeben war. Dies wurde im Rahmen des zweiten Datenschutz Anpassungs- und Umsetzungsgesetz aufgehoben.
- Desweiteren ist zu beachten, dass die Einwilligung in sensible Daten im Sinne des Art. 9 Abs. 1 DSGVO nur dann möglich ist, wenn gem. § 26 Abs. 3 BDSG der ausdrückliche Bezug auf diese vorgenommen wird.

„Pferdefuß“ der datenschutzrechtlichen Einwilligung im Arbeitsverhältnis

Was die Einwilligung im Bereich des Arbeitsrechts angeht, sollte der Betriebsrat bedenken, dass hier regelmäßig keine Waffengleichheit zwischen den Arbeitsvertragsparteien herrscht. Der Bewerber um eine offene Stelle – und häufig auch der Arbeitnehmer, der langfristig seinen Arbeitsplatz erhalten will – wird oft nicht die Möglichkeit haben, der Verarbeitung seiner personenbezogenen Daten zu widersprechen, ohne seine Chancen nachhaltig zu schmälern. Daher sollte der Betriebsrat darauf achten, dass auf die Einwilligung nur in Ausnahmefällen zurückgegriffen wird. Argumentieren kann der Betriebsrat dabei wie folgt: Da der Arbeitnehmer seine Einwilligung (zumindest theoretisch) jederzeit auch wieder widerrufen kann, ist die Einwilligung auch für den Arbeitgeber nicht gerade die allerbeste Möglichkeit, die Datenverarbeitung zu rechtfertigen.

Wann dürfen personenbezogene Daten im Arbeitsverhältnis verarbeitet werden?

Die wichtigste Rechtsgrundlage für Datenverarbeitungen im Beschäftigungsverhältnis ist § 26 BDSG. Danach dürfen:

1. personenbezogene Beschäftigtendaten
2. verarbeitet werden, wenn dies

3. zur Begründung, Durchführung oder Beendigung des Beschäftigtenverhältnisses
4. erforderlich und
5. verhältnismäßig ist.

Beispiele zu § 26 BDSG in der Bewerbungs-/Anbahnungsphase. Unzulässig ist/sind demnach:

- die Erstellung von Persönlichkeitsprofilen,
- Stressinterviews,
- Genomanalysen,
- Graphologische Gutachten, es sei denn der Bewerber hat eingewilligt,
- Frage nach der Gewerkschaftszugehörigkeit,
- Frage nach einer Schwangerschaft (und zwar auch dann, wenn die befristet eingestellte Schwangere aufgrund spezieller Schutzvorschriften während eines Großteils der Vertragslaufzeit nicht arbeiten kann),
- Frage nach politischen oder religiösen Aktivitäten (Ausnahme bei Tendenzunternehmen),
- Frage nach Schulden (sofern diese über ein „normales“ Maß nicht hinausgehen),
- Frage nach Vorstrafen, es sei denn, diese stehen in unmittelbarem Bezug zum Arbeitsverhältnis (z.B. betrügerisch agierender Bankangestellter),
- Frage nach bisherigem Gehalt (die Frage danach ist ausnahmsweise nur dann zulässig, wenn sich daraus ein Hinweis auf die Qualifikation des Bewerbers ergibt).

Werden dem Bewerber unzulässige Fragen gestellt, so hat er diesbezüglich ein „Recht auf Lüge“. Bewerberdaten dürfen nur bis zur Entscheidung über die Nichteinstellung gespeichert werden bzw. so lange, bis Sicherheit besteht, dass daraus keine Rechtsstreitigkeiten (z.B. wegen Verletzung des AGG) entstehen.

Permanente Leistungsüberwachung

Eine permanente Leistungsüberwachung eines Beschäftigten ist nicht zulässig. Sind bestimmte Betriebsräume (z.B. in Banken oder in besonders sicherheitsrelevanten Bereichen) mit Videokameras ausgestattet, so dürfen diese nicht zur dauernden Überwachung der Mitarbeiter dienen (Schwenkbereich oder Bildausschnitt entsprechend wählen!). Entsprechendes gilt bei Aufzeichnungen von Telefongesprächen in Callcentern.

Auch die permanente Überwachung des Aufenthaltsortes von Mitarbeitern durch GPS oder RFID-Chips ist grundsätzlich unzulässig. Ausnahmen können hier in besonders sicherheitsrelevanten Bereichen (z.B. bei Geldtransporten, Rundgang von Wachpersonal) gelten. In all diesen Fällen ist immer die Erforderlichkeit und Verhältnismäßigkeit im Einzelfall zu prüfen.

Speicherung von Stammdaten

Die Speicherung von Stammdaten der Mitarbeiter wie Name, Geschlecht, Familienstand, Schulabschluss, Ausbildung, Studium, Fachrichtung oder Sprachkenntnisse durch den Arbeitgeber ist zulässig. Auch Krankheits- und Fehlzeiten darf der Arbeitgeber speichern, und zwar nicht nur zur Lohn- und Gehaltsabrechnung, sondern auch um festzustellen, inwieweit durch Fehlzeiten das Arbeitsverhältnis

gestört ist (Stichwort: Betriebliches Eingliederungsmanagement und im Extremfall krankheitsbedingte Kündigung).

Telefonate

Bei Telefonaten darf der Arbeitgeber auch äußere Gesprächsdaten wie Tag, Uhrzeit, Beginn und Ende des Telefonats sowie die Zahl der verbrauchten Einheiten erfassen – und zwar unabhängig davon, ob es sich um ein privates oder um ein dienstliches Gespräch handelt. Noch nicht eindeutig geklärt (und wohl eher zu verneinen) ist die Frage, inwieweit die Speicherung der Telefonnummer des Gesprächspartners zulässig ist. Daher sollte nur ein Teil der Telefonnummer gespeichert werden. Die Inhalte von Telefonaten (oder auch Teile davon) dürfen, ohne dass die Gesprächspartner davon in Kenntnis gesetzt wurden, nicht mitgehört oder mitgeschnitten werden. Dies wäre ein Verstoß gegen das „Recht am eigenen Wort“, das aus dem Allgemeinen Persönlichkeitsrechts des Grundgesetzes abgeleitet wird (Entscheidung des Bundesverfassungsgerichts vom 19.12.1991, 1 BvR 382/85).



Tipp: Diese für Telefongespräche entwickelten Grundsätze gelten auch für den E-Mail-Verkehr.

Haftung und Sanktionen im Datenschutzrecht

Die DSGVO und das BDSG sehen eine Reihe von Sanktionen bzw. Bußgeldern vor. Die Vorschriften lassen sich wie folgt unterscheiden:

- Art. 83 Abs. 4 DSGVO sieht bei Verstößen gegen Pflichten des Verantwortlichen, der Auftragsdatenverarbeiter sowie der Zertifizierungs- und Überwachungsstellen eine Geldstrafe in einer Höhe von bis zu 10 Mio. Euro vor. Bei gleichzeitigem Verstoß gegen EU-Wettbewerbsrecht drohen Geldstrafen von bis zu 2 Prozent des weltweiten Vorjahresumsatzes.
- Art. 83 Abs. 5 DSGVO sieht bei Verstößen gegen die Grundsätze für die Verarbeitung, Betroffenenrechte oder Regelungen zur Auslandsdatenverarbeitung eine Geldstrafe in einer Höhe von bis zu 20 Mio. Euro vor. Bei gleichzeitigem Verstoß gegen EU-Wettbewerbsrecht: sind Geldstrafen in einer Höhe von bis zu 4 Prozent weltweiten Vorjahresumsatzes möglich.
- Nach § 43 BDSG können Geldstrafen bis zu einer Höhe von 50.000 Euro verhängt werden, sollte gegen § 30 BDSG (Verbraucherkredite) verstoßen werden.
- Nach § 42 Abs. 1 BDSG droht eine Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe, sollte eine unberechtigte Übermittlung oder Zugänglichmachung nicht allgemein zugänglicher personenbezogener Daten an einen größeren Personenkreis stattgefunden haben.
- Nach § 42 Abs. 2 BDSG kann eine Freiheitsstrafe von bis zu zwei Jahren oder Geldstrafe verhängt werden, sollte eine unberechtigte Verarbeitung nicht allgemein zugänglicher personenbezogener Daten oder Erschleichung nicht allgemein zugänglicher personenbezogener Daten mit Bereicherungs- oder Schädigungsabsicht stattgefunden haben.

Videos zum Thema

Kontakt zur Redaktion

Haben Sie Fragen oder Anregungen? Wenden Sie sich gerne direkt an unsere Redaktion. Wir freuen uns über konstruktives Feedback!

redaktion-dbr@ifb.de

Institut zur Fortbildung von Betriebsräten GmbH & Co. KG © 2025